Комплексна система захисту інформації

Завдання безпеки для військової пошти (20)

Зміст

Зміст

Анотація

Завдання з безпеки для забезпечення конфіденційності, цілісності та гарантованої доставки повідомлень (MHS X.420) з підтримкою грифування.

1. AC

Клас заходів захисту AC — УПРАВЛІННЯ ДОСТУПОМ

Цей клас зосереджується на обмеженні доступу до інформаційних систем, ресурсів та функцій лише для авторизованих користувачів, програм і пристроїв.

Перелік заходів захисту: Забезпечення доступу (AC-3); Управління інформаційними потоками (AC-4); Управління паралельною сесією (AC-10); Атрибути безпеки та приватності (AC-16); Відображення атрибутів на пристроях виведення (AC-16(5)); Диспетчер доступу (AC-25).

1.1. ЗАБЕЗПЕЧЕННЯ ДОСТУПУ (AC-3)

Застосовувати затверджені повноваження для логічного доступу до інформації та ресурсів системи відповідно до чинної політики (правил) управління доступом.

No: 1
Name: ac_3_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Затверджені повноваження на логічний доступ до інформації та ресурсів системи виконуються відповідно до чинних політик(правил) управління доступом

1.2. УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ (AC-4)

Застосувати затверджені повноваження для управління потоком інформації всередині системи та між пов'язаними системами на основі [Призначення: визначеними організацією політиками управління інформаційним потоком].

No: 1
Name: ac_4_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Затверджені повноваження застосовуються для контролю потоку інформації всередині системи та між підключеними системами на основі політики управління інформаційними потоками

No: 2
Name: ac_4_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політики управління інформаційними потоками всередині системи та між підключеними системами

1.3. УПРАВЛІННЯ ПАРАЛЕЛЬНОЮ СЕСІЄЮ (AC-10)

Обмежити кількість одночасних сеансів для кожного [Призначення: визначеного організацією облікового запису та/або типу облікового запису] до [Призначення: визначеної організацією кількості].

No: 1
Name: ac_10_01
Type: integer
Default: 30

Кількість одночасних сеансів для кожного облікового запису та/або типів облікових записів обмежена кількість

No: 2
Name: ac_10_odp_02
Type: integer
Default: 30

Визначено кількість одночасних сеансів, дозволених для кожного облікового запису та/або типу облікового запису

1.4. АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ (AC-16)

a. Визначити засоби для асоціювання (пов'язання) [Призначення: визначених організацією типів атрибутів безпеки та приватності], що приймають [Призначення: визначені організацією значення атрибутів безпеки та приватності] з інформацією, яка зберігається, обробляється та/або передається.
b. Пов'язані атрибути безпеки та приватності мають створюватися і зберігатися разом з інформацією.
c. Встановити дозволені [Призначення: визначені організацією атрибути безпеки] для [Призначення: систем, визначених організацією].
d. Визначити дозволені [Призначення: визначені організацією значення або діапазони] для кожного з встановлених атрибутів безпеки та приватності.

No: 1
Name: ac_16_c_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено типи атрибутів безпеки, які мають бути пов'язані зі значеннями атрибутів безпеки для інформації, що зберігається, обробляється та/або передається; визначено значення атрибутів конфіденційності для типів атрибутів конфіденційності; визначено системи, для яких мають бути встановлені дозволені атрибути безпеки; визначено системи, для яких мають бути встановлені дозволені атрибути конфіденційності; визначено атрибути безпеки, визначені як частина AC-16(a), які дозволені для систем; визначено атрибути конфіденційності, визначені як частина AC-16(a), які дозволені для систем; визначено значення атрибутів або діапазони для встановлених атрибутів; визначено частоту, з якою слід переглядати атрибути безпеки на предмет відповідності; визначено частоту, з якою слід переглядати атрибути конфіденційності на предмет відповідності; надано засоби для асоціювання типів атрибутів безпеки зі значеннями атрибутів безпеки для інформації, що зберігається, обробляється та/або передається надано засоби для асоціювання типів атрибутів конфіденційності зі значеннями атрибутів конфіденційності для інформації, що зберігається, обробляється та/або передається виникають зв'язки з атрибутами; зв'язки атрибутів зберігаються разом з інформацією; на основі атрибутів, визначених у AC-16_ODP[01] для систем, встановлюються наступні дозволені атрибути безпеки: атрибути безпеки; на основі атрибутів, визначених у AC-16_ODP[02] для систем, встановлюються наступні дозволені атрибути приватності: атрибути конфіденційності ; AC-16(d)

No: 2
Name: ac_16_f_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено наступні допустимі значення або діапазони атрибутів для кожного з встановлених атрибутів: значення або діапазони атрибутів; проводиться аудит змін до атрибутів; атрибути безпеки перевіряються на відповідність частота; атрибути конфіденційності перевіряються на відповідність частота

No: 3
Name: ac_16_odp_02
Type: string
Default: nil

Визначено типи атрибутів конфіденційності, які мають бути пов'язані зі значеннями атрибутів конфіденційності для інформації, що зберігається, обробляється та/або передається

No: 4
Name: ac_16_odp_03
Type: string
Default: nil

Визначено значення атрибутів безпеки для типів атрибутів безпеки

1.4.1. ВІДОБРАЖЕННЯ АТРИБУТІВ НА ПРИСТРОЯХ ВИВЕДЕННЯ (AC-16(5))

Відображати атрибути безпеки та приватності в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати [Призначення: визначені організацією спеціальні інструкції щодо поширення, обробки чи наступного розподілу інформації], використовуючи [Призначення: визначену організацією ідентифікацію, у зручній для людини формі про стандартні угоди про присвоєння імен].

No: 1
Name: ac_16_5_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Для кожного об'єкта, який система передає на пристрої виведення, визначено спеціальні інструкції щодо поширення, обробки чи розподілу, які мають використовуватися; визначено стандартні угоди про ідентифікацію атрибутів безпеки та конфіденційності, які повинні відображатися в зручній для читання формі на кожному об'єкті, який система передає на пристрої виводу; атрибути безпеки відображаються у формі, зручній для читання людиною, на кожному об'єкті, який система передає на пристрої виводу для ідентифікації інструкцій з використанням угод про іменування; атрибути конфіденційності відображаються у формі, зручній для читання людиною, на кожному об'єкті, який система передає на пристрої виводу для ідентифікації інструкцій з використанням угод про іменування

1.5. ДИСПЕТЧЕР ДОСТУПУ (AC-25)

Впровадити диспетчер доступу для [Призначення: визначеної організацією політики контролю доступу], який захищений від несанкціонованого доступу, завжди був доступний для виклику та досить компактний, щоб бути підданим аналізу й тестуванню, надійність якого може бути гарантована.

No: 1
Name: ac_25_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Реалізовано диспетчер доступу для політики контролю доступу, який захищений від несанкціонованого доступу, завжди доступний для виклику та досить компактний, щоб бути підданим аналізу й тестуванню, надійність якого може бути гарантована

No: 2
Name: ac_25_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політики контролю доступу, для яких реалізовано диспетчер доступу

2. AU

Клас заходів захисту AU — АУДИТ ТА ПІДЗВІТНІСТЬ

Цей клас забезпечує можливість відстеження дій у системі, генерування, захист та аналіз записів аудиту для виявлення порушень політики безпеки.

Перелік заходів захисту: Події аудиту (AU-2); Неспростовність (AU-10); Цифрові підписи (AU-10(5)); Генерація даних аудиту (AU-12).

2.1. ПОДІЇ АУДИТУ (AU-2)

a. Визначити типи подій, які система може реєструвати для підтримки функції аудиту: [Призначення: типи подій, визначені організацією, які система здатна реєструвати];
b. Координувати функції аудиту безпеки з іншими організаційними підрозділами, які вимагають інформації, пов'язаної з аудитом, для посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються;
c. Визначити, які типи подій підлягають аудиту: [Призначення: визначені організацією події, що підлягають аудиту (підмножина подій, що підлягають аудиту, визначених в AU-2 a.), а також частота (або ситуація, що вимагає) проведення аудиту для кожної ідентифікованої події]
d. Обґрунтувати, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та приватністю;
e. Перегляньте й оновіть типи подій, вибрані для журналювання [Призначення: частота, визначена організацією].

No: 1
Name: au_2_a
Type: string
Default: nil

Типи подій, які система здатна реєструвати, визначено для підтримки функції аудиту

No: 2
Name: au_2_b
Type: string
Default: nil

Функція аудиту безпеки координується з іншими підрозділами організації, які вимагають інформації, пов'язаної з аудитом, длдля посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються

No: 3
Name: au_2_c_01
Type: string
Default: nil

Типи подій (підмножина 02_ODP[01]) визначаються для реєстрації у системі; AU-

No: 4
Name: au_2_c_02
Type: string
Default: "щорічно"

Зазначені типи подій реєструються 02_ODP[03] частота або ситуація>; <AU-

No: 5
Name: au_2_d

Type: string
Default: nil

Надається обґрунтування, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та конфіденційністю

No: 6
Name: au_2_e
Type: string
Default: "щорічно"

Переглядаються та оновлюються типи подій, вибрані для реєстрації, частота. у системі

No: 7
Name: au_2_odp_01
Type: string
Default: nil

Визначено типи подій, які система може реєструвати для підтримки функції аудиту

No: 8
Name: au_2_odp_02
Type: string
Default: nil

Визначено типи подій (підмножина AU-02_ODP[01]) що підлягають аудиту у системі

No: 9
Name: au_2_odp_03
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено частоту або ситуацію, що вимагає проведення аудиту для кожної ідентифікованої події

No: 10
Name: au_2_odp_04
Type: string
Default: "щорічно"

Частота перегляду та оновлення типів подій, обраних для журналювання

2.2. НЕСПРОСТОВНІСТЬ (AU-10)

Надавайте неспростовні докази того, що особа (або процес, який діє від імені особи) виконала [Призначення: дії, визначені організацією, на які поширюється принцип неспростовності].

No: 1
Name: au_10_01
Type: list
Default: ["admin", "security_officer"]

Надаються неспростовні докази того, що особа (або процес, що діє від імені особи) виконала дії

No: 2
Name: au_10_odp
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено дії, на які поширюється принцип неспростовності

2.2.1. ЦИФРОВІ ПІДПИСИ (AU-10(5))

No: 1
Name: au_10_5_01
Type: string
Default: nil

НЕСПРОСТОВНІСТЬ - ЦИФРОВІ ПІДПИСИ [Вилучено: Включено до SI-07]

2.3. ГЕНЕРАЦІЯ ДАНИХ АУДИТУ (AU-12)

a. Забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2a в [Призначення: визначених організацією компонентах системи].
b. Дозволити [Призначення: визначеному організацією персоналу або посадам] вибирати, які типи подій, що перевіряються, повинні перевірятися окремими компонентами системи;
c. Генерувати записи аудиту для типів подій, визначених в AU-2c. з вмістом згідно з AU-3.

No: 1
Name: au_12_a
Type: string
Default: nil

Можливість генерації записів аудиту для типів подій, які система здатна перевіряти (визначених у AU-02_ODP[01]), забезпечується компонентами системи

No: 2
Name: au_12_b
Type: list
Default: ["admin", "security_officer"]

Персонал або ролі може/можуть вибирати типи подій, які будуть реєструватися певними компонентами системи; AU-12(c) згенеровано записи аудиту для типів подій, визначених у AU02_ODP[02], які включають вміст записів аудиту, визначений у AU03

No: 3
Name: au_12_odp_01
Type: string
Default: nil

Визначено компоненти системи, які забезпечують можливість генерації записів аудиту для типів подій (визначених у AU02_ODP[02])

No: 4
Name: au_12_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, яким дозволено обирати типи подій, що мають реєструватися певними компонентами системи

3. CM

Клас заходів захисту CM — УПРАВЛІННЯ КОНФІГУРАЦІЄЮ

Цей клас гарантує створення та підтримання базових налаштувань системи, а також строгий контроль за змінами в апаратному та програмному забезпеченні.

Перелік заходів захисту: Обмеження доступу до зміни (CM-5).

3.1. ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ (CM-5)

Визначити, задокументувати, затвердити та забезпечити застосування фізичних і логічних обмежень доступу, пов'язаних зі змінами в системі.

No: 1
Name: cm_5_01
Type: string
Default: nil

Визначені та задокументовані фізичні обмеження доступу, пов'язані зі змінами в системі

No: 2
Name: cm_5_02
Type: string
Default: nil

Затверджені фізичні обмеження доступу, пов'язані зі змінами в системі

No: 3
Name: cm_5_03
Type: string
Default: nil

Застосовуються фізичні обмеження доступу, пов'язані зі змінами в системі

No: 4
Name: cm_5_04
Type: string
Default: nil

Визначені та задокументовані логічні обмеження доступу, пов'язані зі змінами в системі

No: 5
Name: cm_5_05
Type: string
Default: nil

Затверджені логічні обмеження доступу, пов'язані зі змінами в системі

No: 6
Name: cm_5_06
Type: string
Default: nil

Застосовуються логічні обмеження доступу, пов'язані зі змінами в системі

4. IA

Клас заходів захисту IA — ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

Цей клас відповідає за однозначне розпізнавання користувачів або пристроїв та підтвердження їхньої справжності перед наданням доступу до системи.

Перелік заходів захисту: ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS) (IA-2(12)); Автентифікація на основі апаратних токенів (IA-5(11)).

4.0.1. ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS) (IA-2(12))

No: 1
Name: ia_2_12_01
Type: list
Default: ["admin", "security_officer"]

Приймаються та електронним шляхом підтверджуються повноваження облікових даних особистої ідентифікації

4.0.2. АВТЕНТИФІКАЦІЯ НА ОСНОВІ АПАРАТНИХ ТОКЕНІВ (IA-5(11))

No: 1
Name: ia_5_11_01
Type: string
Default: nil

УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ АПАРАТНИХ ТОКЕНІВ [Вилучено: Включено до IA-02(01), IA-02(02)]

5. MP

Клас заходів захисту MP — ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ

Цей клас спрямований на безпечне зберігання, транспортування, використання та знищення як цифрових, так і паперових носіїв інформації.

Перелік заходів захисту: Знищення інформації на носіях інформації (MP-6); Таємна інформація (MP-8(4)).

5.1. ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ (MP-6)

a. Очищувати [Призначення: визначені організацією системні носії] перед утилізацією, випуском за межі організаційного контролю, або перед повторним використанням [Призначення: методами та процедурами очищення, визначеними організацією].
b. Використовувати механізми очищення зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.

No: 1
Name: mp_6_a_01
Type: string
Default: nil

Носії інформації системи перед утилізацією піддаються очищенню за допомогою методів та процедур очищення

No: 2
Name: mp_6_a_02
Type: string
Default: nil

Носії інформації системи очищаються за допомогою методів та процедур очищення перед випуском за межі контрольованої зони

No: 3
Name: mp_6_a_03
Type: string
Default: nil

Носії інформації системи очищуються за допомогою методів і процедур очищення перед повторним використанням

No: 4
Name: mp_6_b
Type: string
Default: "автоматизований засіб моніторингу"

Застосовуються механізми очищення, надійність і цілісність яких відповідає категорії безпеки або рівню секретності інформації

No: 5
Name: mp_6_odp_01
Type: string
Default: nil

Визначено носії інформації системи, які підлягають очищенню перед утилізацією

No: 6
Name: mp_6_odp_02
Type: string
Default: nil

Визначено носії інформації системи, які підлягають очищенню перед випуском за межі контрольованої зони

No: 7
Name: mp_6_odp_03
Type: string
Default: nil

Визначені носії інформації системи, що підлягають очищенню перед повторним використанням

No: 8
Name: mp_6_odp_04
Type: string
Default: nil

Визначено методи та процедури очищення, які слід використовувати для очищення перед утилізацією

No: 9
Name: mp_6_odp_05
Type: string
Default: nil

Визначено методи та процедури очищення, які слід використовувати для очищення перед випуском за межі контрольованої зони

No: 10
Name: mp_6_odp_06
Type: string
Default: nil

Визначено методи та процедури очищення, які слід використовувати для очищення перед повторним використанням

5.1.1. ТАЄМНА ІНФОРМАЦІЯ (MP-8(4))

No: 1
Name: mp_8_4_01
Type: string
Default: nil

Ідентифіковано носії інформації, що містять інформацію з обмеженим доступом

No: 2
Name: mp_8_4_02
Type: list
Default: ["admin", "security_officer"]

Носії інформації, що містять інформацію з обмеженим доступом, знижуються в класі перед передачею особам, які не мають необхідних дозволів на доступ

6. SC

Клас заходів захисту SC — ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА

Цей клас охоплює механізми захисту інформації під час її передачі мережами зв'язку, криптографічний захист та ізоляцію критичних компонентів.

Перелік заходів захисту: Конфіденційність та криптографічний захист (SC-8(1)); Попередня і постобробка (SC-8(2)); Встановлення ключами (SC-12); Сертифікати інфраструктури відкритих ключів (SC-17); ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ | КРИПТОГРАФІЧНИЙ ЗАХИСТ.

6.0.1. КОНФІДЕНЦІЙНІСТЬ ТА КРИПТОГРАФІЧНИЙ ЗАХИСТ (SC-8(1))

No: 1
Name: sc_8_1_odp
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {запобігти несанкціонованому розголошенню інформації; виявити зміни в інформації}

6.0.2. ПОПЕРЕДНЯ І ПОСТОБРОБКА (SC-8(2))

No: 1

Name: sc_8_2_01
Type: string
Default: nil

КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПОПЕРЕДНЯ І ПОСТОБРОБКА МЕТА ОЦІНКИ: Визначити, чи:

No: 2
Name: sc_8_2_odp
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {конфіденційність; цілісність}

6.1. ВСТАНОВЛЕННЯ КЛЮЧАМИ (SC-12)

Встановити та управляти криптографічними ключами для криптографічних засобів, які використовуються в системі відповідно до [Призначення: визначені організацією вимоги до генерації, поширення, зберігання, доступу та знищення ключів].

No: 1
Name: sc_12_01
Type: string
Default: "AES-256-GCM"

Встановлюються криптографічні ключі, коли в системі використовується криптографія відповідно до < SC-12_ ODP вимог >

No: 2
Name: sc_12_02
Type: string
Default: "AES-256-GCM"

Здійснюється управління криптографічними ключами, коли в системі використовується криптографія, відповідно до вимог

No: 3
Name: sc_12_odp
Type: string
Default: nil

Визначені вимоги до генерації, розповсюдження, зберігання, доступу та знищення ключів

6.2. СЕРТИФІКАТИ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ (SC-17)

a. Випускати сертифікати відкритого ключа відповідно до [Призначення: визначеної організацією політики сертифікації];
b. Отримувати сертифікати відкритого ключа від затвердженого постачальника послуг.

Немає параметрів для цього контролю.

6.2.1. ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ | КРИПТОГРАФІЧНИЙ ЗАХИСТ

No: 1
Name: sc_28_1_01
Type: string
Default: "AES-256-GCM"

Реалізовані криптографічні механізми для запобігання несанкціонованому розкриттю інформації, що знаходиться в стані спокою на системних компонентах або носіях

No: 2
Name: sc_28_1_02
Type: string
Default: "AES-256-GCM"

Реалізовані криптографічні механізми для запобігання несанкціонованій модифікації інформації, що знаходиться в стані спокою на системних компонентах або носіях